FDA warns public of continued extortion scam by FDA impersonators

FDA NEWS RELEASE

For Immediate Release: Jan. 7, 2011

Media Inquiries: Christopher Kelly, 301-796-4676 christopher.kelly@fda.hhs.gov

Consumer Inquiries: 888-INFO-FDA

The U.S. Food and Drug Administration is warning the public about criminals posing as FDA special agents and other law enforcement personnel as part of a continued international extortion scam.

The criminals call the victims -- who in most cases previously purchased drugs over the Internet or via "telepharmacies" -- and identify themselves as FDA special agents or other law enforcement officials. The criminals inform the victims that purchasing drugs over the Internet or the telephone is illegal, and that law enforcement action will be pursued unless a fine or fee ranging from $100 to $250,000 is paid. Victims often also have fraudulent transactions placed against their credit cards.

The criminals always request the money be sent by wire transfer to a designated location, usually in the Dominican Republic. If victims refuse to send money, they are often threatened with a search of their property, arrest, deportation, physical harm and/or incarceration.

"Impersonating an FDA official is a violation of federal law," said Dara Corrigan, the FDA's associate commissioner for regulatory affairs. "FDA special agents and other law enforcement officials are not authorized to impose or collect criminal fines. Only a court can take such action."

In most instances, victims of extortion-related calls have also received telephone solicitations for additional pharmaceutical purchases from other possibly related, illegal entities located overseas. The extortionists use customer lists complete with extensive personal information provided through previous purchase transactions. These include names, addresses, telephone numbers, Social Security numbers, dates of birth, purchase histories and credit card account numbers

Typically, these criminals use telephone numbers that change constantly and make it appear as though their calls originate in the United States.

No known victim has been approached in person by a law enforcement impersonator associated with this scheme.

The FDA's Office of Criminal Investigations, with the U.S. Drug Enforcement Administration, and the U.S. Immigrations and Customs Enforcement, Homeland Security Investigations, with the support of various U.S. Attorneys, are pursuing multiple national and international criminal investigations.

Arrests have been made and additional prosecutions are pending; however, the scheme is likely to continue. The FDA has issued similar warnings in the past:

§ FDA Warns Public of Extortion Scam by FDA Impersonators1 (11/12/2008)

§ FDA Warns Public of Continued Extortion Scam by FDA Impersonators2 (12/29/2009)

Victims of this scheme who have suffered monetary loss through the payment of funds in response to an extortion call from a person purporting to be an FDA or other law enforcement official regarding illegal pharmaceutical transactions may obtain a victim questionnaire by contacting the FDA's Office of Criminal Investigations3 and clicking "Report Suspected Criminal Activity.

Anyone receiving a purported official document on agency letterhead may verify its authenticity by contacting that organization directly via a publicly available phone number. Additionally, all federal agencies use email addresses with a "gov" email extension.

The FDA also reminds consumers that pharmaceutical products offered online and by telephone by sources of unknown origin can pose a substantial health risk. Products recovered during this investigation that were purchased from online or telephone sources have been found to contain trace amounts of heroin, other undisclosed and potentially harmful active pharmaceutical ingredients, or no active ingredient at all. Purchases should only be made from licensed pharmacies located in the United States. In addition to the increased risk of purchasing unsafe and ineffective drugs from Web sites operating outside the law, personal data may be compromised.

For more on unlawful drug sales on the Internet, see Protecting Yourself4.

Questions and Answers

How did these people obtain my information?

They likely obtained the victim's information based on a previous online or telepharmacy transaction, or from a submitted medical questionnaire. These instances could have occurred years ago, with personal information now on customer lists trafficked by these criminal groups. These customer lists can contain tens of thousands of names and a substantial amount of self-reported data provided by consumers during previous transactions. Typically, victims are being contacted by multiple unrelated groups, often for different purposes. (extortion, selling illegal pharmaceuticals, etc.)

How do I make the calls stop?

The extorters, just like the majority of telephone solicitors for illegal prescription medication, are based overseas and use voice over internet protocol (VOIP) telephone numbers, most commonly "Magic Jack". These services provide the extorters with the flexibility to constantly change their phone numbers and select ones with U.S. area codes. If the victims change whatever number(s) were used to contact them, and do not engage in any additional risky pharmaceutical transactions, the threatening phone calls and associated telephone solicitations for pharmaceuticals should cease.

What proactive steps can victims take?

Individuals who purchase medication online or via tele-pharmacies are frequently victims of credit card fraud, since this is how the medication is often purchased. Victims may want to consider alerting their applicable financial institutions to ensure that identity theft has not occurred.

Why is FDA only asking victims who have lost money to contact the agency?

The most effective way to track these criminals is to investigate the permanent record established when money transfers take place.

Have individuals been arrested?

Yes. However, this scheme will likely not be eradicated and instead will continue to evolve. For example, the extorters now occasionally reference other countries, such as Costa Rica, instead of the DR, as means to avoid all of the publicity regarding this scheme.

Am I going to be able to get my money back?

In almost all instances victims will not be able to recoup losses. Multiple criminal groups employ this scheme, principally from overseas, and large monetary seizures are not anticipated.

Am I in danger?

In terms of physical danger, no victim has ever been approached in person, and the vast majority of these callers, regardless of their intent, are based overseas. Their use of "police-type scanners", law enforcement language and fictitious documents are attempts at a false sense of legitimacy. Extorters also occasionally reference cars parked on a victim's street -- information that can be obtained online at various Web sites, as a way to frighten individuals into believing the extorters are near their residence. If an individual feels threatened for his or her personal safety, immediately contact the appropriate local enforcement agency

Is it possible that these callers are part of some "secret" investigative group, and FDA is just not aware of it?

No. Law enforcement officials from both the U.S. and the Dominican Republic are pursuing these criminals. More information regarding this scheme is available on FDA and DEA Web sites, or through online searches. Extradition proceedings between countries require close cooperation and often a formal treaty, and this often takes an extended period of time to complete.